i) uneingeschränkte Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens oder eines beauftragten Dritten und der zuständigen Behörde sowie das Recht auf Anfertigung von Kopien einschlägiger Unterlagen vor Ort, wenn ihnen für die Geschäftstätigkeit des IKT-Drittdienstleisters entscheidende Bedeutung zukommt, wobei die tatsächliche Ausübung dieser Rechte nicht durch andere vertragliche Vereinbarungen oder Umsetzungsrichtlinien behindert oder eingeschränkt wird;

ii) das Recht, alternative Bestätigungsniveaus zu vereinbaren, wenn die Rechte anderer Kunden betroffen sind;

iii) die Verpflichtung des IKT-Drittdienstleisters zur uneingeschränkten Zusammenarbeit bei Vor-Ort-Inspektionen und Audits, die von den zuständigen Behörden, der federführenden Überwachungsbehörde, dem Finanzunternehmen oder einem beauftragten Dritten durchgeführt werden; und

iv) die Verpflichtung, Einzelheiten zu Umfang und Häufigkeit dieser Inspektionen sowie dem dabei zu befolgenden Verfahren mitzuteilen;

f) Ausstiegsstrategien, insbesondere die Festlegung eines verbindlichen angemessenen Übergangszeitraums,

i) in dem der IKT-Drittdienstleister weiterhin die entsprechenden Funktionen oder IKT-Dienstleistungen bereitstellt, um das Risiko von Störungen im Finanzunternehmen zu verringern oder um dessen geordnete Abwicklung und Umstrukturierung sicherzustellen;

ii) der dem Finanzunternehmen ermöglicht, zu einem anderen IKT-Drittdienstleister zu wechseln oder auf interne Lösungen umzustellen, die der Komplexität der erbrachten Dienstleistung entsprechen.

Abweichend von Buchstabe e können der IKT-Drittdienstleister und das Finanzunternehmen, das ein Kleinstunternehmen ist, vereinbaren, dass die Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens auf einen unabhängigen Dritten übertragen werden können, der vom IKT-Drittdienstleister benannt wird, sowie dass das Finanzunternehmen von diesem Dritten jederzeit Informationen und Gewähr in Bezug auf die Leistung des IKT-Drittdienstleisters verlangen kann.

(4) Bei der Aushandlung vertraglicher Vereinbarungen erwägen Finanzunternehmen und IKT-Drittdienstleister die Verwendung von Standardvertragsklauseln, die von Behörden für bestimmte Dienstleistungen entwickelt wurden.

(5) Die ESA erarbeiten über den Gemeinsamen Ausschuss Entwürfe technischer Regulierungsstandards, um die in Absatz 2 Buchstabe a genannten Aspekte zu präzisieren, die ein Finanzunternehmen bei der Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen bestimmen und bewerten muss.

Bei der Ausarbeitung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte.

Die ESA übermitteln der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Juli 2024.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme der in Unterabsatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

Abschnitt II

Überwachungsrahmen für kritische IKT-Drittdienstleister

Artikel 31

Einstufung kritischer IKT-Drittdienstleister

(1) Die ESA nehmen über den Gemeinsamen Ausschuss und auf Empfehlung des gemäß Artikel 32 Absatz 1 eingerichteten Überwachungsforums folgende Aufgaben wahr:

a) Einstufung der IKT-Drittdienstleister, die für Finanzunternehmen kritisch sind, nachdem eine entsprechende Bewertung unter Berücksichtigung der in Absatz 2 genannten Kriterien durchgeführt wurde;

b) Ernennung derjenigen Europäischen Aufsichtsbehörde zur federführenden Überwachungsbehörde für jeden kritischen IKT-Drittdienstleister, die gemäß den Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 bzw. (EU) Nr. 1095/2010 für diejenigen Finanzunternehmen zuständig ist, die nachweislich der Summe der einzelnen Bilanzen dieser Finanzunternehmen zusammen den größten Anteil des Gesamtvermögens am Gesamtwert der Aktiva aller Finanzunternehmen halten, die die Dienste des betreffenden kritischen IKT-Drittdienstleisters nutzen.

(2) Die Einstufung nach Absatz 1 Buchstabe a basiert in Bezug auf IKT-Dienstleistungen, die vom IKT-Drittdienstleister bereitgestellt werden, auf den folgenden Kriterien:

a) den systemischen Auswirkungen auf die Stabilität, Kontinuität oder Qualität der Erbringung von Finanzdienstleistungen, falls der betreffende IKT-Drittdienstleister bei der Erbringung seiner Dienste einer umfassenden Betriebsstörung ausgesetzt wäre, wobei die Zahl von Finanzunternehmen und der Gesamtwert der Aktiva derjenigen Finanzunternehmen zu berücksichtigen ist, für die der betreffende IKT-Drittdienstleister Dienstleistungen erbringt;

b) dem systemischen Charakter oder der Bedeutung der Finanzunternehmen, die auf den jeweiligen IKT-Drittdienstleister zurückgreifen, bewertet anhand der folgenden Parameter:

   i) der Anzahl global systemrelevanter Institute (G-SRI) oder anderer systemrelevanter Institute (A-SRI), die auf den jeweiligen IKT-Drittdienstleister zurückgreifen;

   ii) der Interdependenz zwischen den unter Ziffer i genannten G-SRI oder A-SRI und anderen Finanzunternehmen, einschließlich der Fälle, in denen die G-SRI oder A-SRI Finanzinfrastrukturdienstleistungen für andere Finanzunternehmen erbringen;

c) der Abhängigkeit von Finanzunternehmen von den Dienstleistungen des betreffenden IKT-Drittdienstleisters mit Blick auf kritische oder wichtige Funktionen von Finanzunternehmen, in die letztlich derselbe IKT-Drittdienstleister involviert ist — unabhängig davon, ob Finanzunternehmen diese Dienste direkt oder indirekt durch Vereinbarungen über die Unterauftragsvergabe in Anspruch nehmen;

d) dem Grad der Substituierbarkeit des IKT-Drittdienstleisters unter Berücksichtigung der folgenden Parameter:

   i) des Mangels an echten, auch teilweisen Alternativen aufgrund der begrenzten Zahl von IKT-Drittdienstleistern, die auf einem bestimmten Markt tätig sind, oder des Marktanteils des betreffenden IKT-Drittdienstleisters oder der damit verbundenen technischen Komplexität oder Differenziertheit, auch in Bezug auf proprietäre Technologien, oder der besonderen Merkmale der Organisation oder Tätigkeit des IKT-Drittdienstleisters;

   ii) der Schwierigkeiten bei der teilweisen oder vollständigen Migration der einschlägigen Daten und Arbeitslasten vom jeweiligen IKT-Drittdienstleister zu einem anderen IKT-Drittdienstleister, die entweder auf erhebliche finanzielle Kosten, zeitliche oder sonstige Ressourcen, die der Migrationsprozess mit sich bringen kann, oder auf erhöhte IKT-Risiken oder sonstige operationelle Risiken zurückzuführen sind, denen das Finanzunternehmen durch eine solche Migration ausgesetzt sein könnte.

(3) Gehört der IKT-Drittdienstleister zu einer Gruppe, so werden die in Absatz 2 genannten Kriterien in Bezug auf die von der Gruppe als Ganzes bereitgestellten IKT-Dienstleistungen berücksichtigt.

(4) Kritische IKT-Drittdienstleister, die Teil einer Gruppe sind, benennen eine juristische Person als Koordinierungsstelle, um eine angemessene Vertretung und Kommunikation mit der federführenden Überwachungsbehörde sicherzustellen.

(5) Die federführende Überwachungsbehörde unterrichtet den IKT-Drittdienstleister über das Ergebnis der Bewertung, die zu der in Absatz 1 Buchstabe a genannten Einstufung geführt hat. Innerhalb von sechs Wochen ab dem Datum der Unterrichtung kann der IKT-Drittdienstleister der federführenden Überwachungsbehörde eine begründete Erklärung mit allen für die Zwecke der Bewertung relevanten Informationen übermitteln. Die federführende Überwachungsbehörde prüft die begründete Erklärung und kann verlangen, dass innerhalb von 30 Kalendertagen nach Eingang der Erklärung zusätzliche Informationen übermittelt werden.

Nach der Einstufung eines IKT-Drittdienstleisters als kritisch, unterrichten die ESA den IKT-Drittdienstleister über den Gemeinsamen Ausschuss über diese Einstufung und das Anfangsdatum, ab dem er tatsächlich Überwachungstätigkeiten unterliegen wird. Dieses Anfangsdatum darf nicht mehr als einen Monat nach der Unterrichtung liegen. Der IKT-Drittdienstleister teilt den Finanzunternehmen, für die er Dienstleistungen erbringt, seine Einstufung als kritisch mit.

(6) Der Kommission wird die Befugnis übertragen, gemäß Artikel 57 einen delegierten Rechtsakt zu erlassen, um diese Verordnung durch die weitere Präzisierung der in Absatz 2 genannten Kriterien bis 17. Juli 2024 zu ergänzen.

(7) Die Einstufung nach Absatz 1 Buchstabe a darf erst angewendet werden, wenn die Kommission einen delegierten Rechtsakt gemäß Absatz 6 erlassen hat.

(8) Die Einstufung nach Absatz 1 Buchstabe a gilt nicht für:

i) Finanzunternehmen, die IKT-Dienstleistungen für andere Finanzunternehmen bereitstellen;

ii) IKT-Drittdienstleister, die Überwachungsrahmen unterliegen, die zur Unterstützung der in Artikel 127 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union genannten Aufgaben eingerichtet wurden;

iii) gruppeninterne IKT-Dienstleister;

iv) IKT-Drittdienstleister, die IKT-Dienstleistungen ausschließlich in einem Mitgliedstaat für Finanzunternehmen bereitstellen, die nur in diesem Mitgliedstaat tätig sind.

(9) Die ESA erstellen, veröffentlichen und aktualisieren die Liste kritischer IKT-Drittdienstleister auf Unionsebene jährlich über den Gemeinsamen Ausschuss.

(10) Die zuständigen Behörden übermitteln dem gemäß Artikel 32 eingerichteten Überwachungsforum für die Zwecke von Absatz 1 Buchstabe a die in Artikel 28 Absatz 3 Unterabsatz 3 genannten Berichte auf jährlicher und aggregierter Basis. Das Überwachungsforum bewertet die Abhängigkeiten von Finanzunternehmen gegenüber IKT-Drittdienstleistern auf der Grundlage der von den zuständigen Behörden übermittelten Informationen.

(11) Diejenigen IKT-Drittdienstleister, die nicht in der in Absatz 9 genannten Liste aufgeführt sind, können beantragen, gemäß Absatz 1 Buchstabe a als kritisch eingestuft zu werden.

Für die Zwecke von Unterabsatz 1 reicht der IKT-Drittdienstleister bei der EBA, der ESMA oder der EIOPA einen begründeten Antrag ein, die über den Gemeinsamen Ausschuss entscheiden, ob dieser IKT-Drittdienstleister gemäß Absatz 1 Buchstabe a als kritisch eingestuft werden soll.

Die in Unterabsatz 2 genannte Entscheidung wird innerhalb von 6 Monaten nach Eingang des Antrags getroffen und dem IKT-Drittdienstleister mitgeteilt.

(12) Finanzunternehmen dürfen nur dann die Dienstleistungen eines IKT-Drittdienstleisters mit Sitz in einem Drittland in Anspruch nehmen, der gemäß Absatz 1 Buchstabe a als kritisch eingestuft worden ist, wenn er innerhalb von zwölf Monaten nach der Einstufung ein Tochterunternehmen in der Union gegründet hat.

(13) Der in Absatz 12 genannte kritische IKT-Drittdienstleister teilt der federführenden Überwachungsbehörde jede Änderung der Leitungsstruktur des in der Union niedergelassenen Tochterunternehmens mit.

Artikel 32

Struktur des Überwachungsrahmens

(1) Der Gemeinsame Ausschuss richtet gemäß Artikel 57 Absatz 1 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 das Überwachungsforum als Unterausschuss ein, der die Arbeit des Gemeinsamen Ausschusses und der in Artikel 31 Absatz 1 Buchstabe b genannten federführenden Überwachungsbehörde im Bereich des IKT-Drittparteienrisikos in allen Finanzsektoren unterstützt. Das Überwachungsforum erarbeitet die Entwürfe gemeinsamer Positionen und gemeinsamer Maßnahmen des Gemeinsamen Ausschusses in diesem Bereich.

Das Überwachungsforum erörtert regelmäßig einschlägige Entwicklungen in Bezug auf IKT-Risiken und -Schwachstellen und fördert einen kohärenten Ansatz bei der Überwachung des IKT-Drittparteienrisikos auf Unionsebene.

(2) Das Überwachungsforum führt jährlich eine gemeinsame Bewertung der Ergebnisse und Erkenntnisse der Überwachungstätigkeiten durch, die für alle kritischen IKT-Drittdienstleister durchgeführt wurden, und fördert Koordinierungsmaßnahmen, um die digitale operationale Resilienz von Finanzunternehmen zu erhöhen, bewährte Verfahren zum Angehen des IKT-Konzentrationsrisikos zu fördern und Möglichkeiten zur Abschwächung sektorübergreifender Risikotransfers zu untersuchen.

(3) Das Überwachungsforum legt umfassende Referenzwerte für kritische IKT-Drittdienstleister vor, die vom Gemeinsamen Ausschuss als gemeinsame Positionen der ESA gemäß Artikel 56 Absatz 1 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 anzunehmen sind.

(4) Das Überwachungsforum setzt sich zusammen aus

a) den Vorsitzenden der ESA;

b) einem hochrangigen Vertreter des aktuellen Personals der in Artikel 46 genannten betreffenden zuständigen Behörde eines jeden Mitgliedstaats;

c) den Exekutivdirektoren jeder Europäischen Aufsichtsbehörde und einem Vertreter der Kommission, des ESRB, der EZB und der ENISA als Beobachter;

d) gegebenenfalls einem zusätzlichen Vertreter einer in Artikel 46 genannten zuständigen Behörde eines jeden Mitgliedstaats als Beobachter;

e) gegebenenfalls einem Vertreter der gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden, der für die Beaufsichtigung eines wesentlichen oder wichtigen, von der genannten Richtlinie erfassten Unternehmens, das als kritischer IKT-Drittdienstleister eingestuft wurde, zuständig ist, als Beobachter.

Das Überwachungsforum kann gegebenenfalls den Rat unabhängiger Sachverständiger einholen, die gemäß Absatz 6 ernannt wurden.

(5) Jeder Mitgliedstaat benennt die jeweils zuständige Behörde, deren Mitarbeiter der in Absatz 4 Unterabsatz 1 Buchstabe b genannte hochrangige Vertreter ist, und setzt die federführende Überwachungsbehörde davon in Kenntnis.

Die ESA veröffentlichen auf ihrer Website die Liste der von den Mitgliedstaaten benannten hochrangigen Vertreter aus dem aktuellen Personal der jeweils zuständigen Behörde.

(6) Die in Absatz 4 Unterabsatz 2 genannten unabhängigen Sachverständigen werden vom Überwachungsforum aus einem Pool von Sachverständigen ernannt, die im Anschluss an ein öffentliches und transparentes Bewerbungsverfahren ausgewählt wurden.

Die unabhängigen Sachverständigen werden auf der Grundlage ihres Fachwissens in den Bereichen Finanzstabilität, digitale operationale Resilienz und Fragen der IKT-Sicherheit ernannt. Sie handeln unabhängig und objektiv im alleinigen Interesse der Union als Ganzes und dürfen von Organen oder Einrichtungen der Union, von der Regierung eines Mitgliedstaats oder von öffentlichen oder privaten Stellen Weisungen weder einholen noch entgegennehmen.

(7) Gemäß Artikel 16 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 geben die ESA für die Zwecke dieses Abschnitts bis zum 17. Juli 2024 Leitlinien für die Zusammenarbeit zwischen den ESA und den zuständigen Behörden heraus, die die detaillierten Verfahren und Bedingungen für die Zuweisung und Ausführung von Aufgaben zwischen zuständigen Behörden und den ESA sowie die Einzelheiten zum Austausch von Informationen regeln, die zuständige Behörden benötigen, um die Weiterbehandlung der in Artikel 35 Absatz 1 Buchstabe d genannten Empfehlungen zu gewährleisten, die an kritische IKT-Drittdienstleister gerichtet werden.

(8) Die in diesem Abschnitt dargelegten Anforderungen gelten unbeschadet der Anwendung der Richtlinie (EU) 2022/2555 und anderer Überwachungsvorschriften der Union, die für Anbieter von Cloud-Computing-Diensten gelten.

(9) Die ESA legen dem Europäischen Parlament, dem Rat und der Kommission über den Gemeinsamen Ausschuss und auf der Grundlage von Vorarbeiten des Überwachungsforums jährlich einen Bericht über die Anwendung dieses Abschnitts vor.

Artikel 33

Aufgaben der federführenden Überwachungsbehörde

(1) Die gemäß Artikel 31 Absatz 1 Buchstabe b ernannte federführende Überwachungsbehörde führt die Überwachung über die zugewiesenen kritischen IKT-Drittdienstleister durch und ist für diese kritischen IKT-Drittdienstleister für die Zwecke aller mit der Überwachung verbundenen Angelegenheiten die vorrangige Anlaufstelle.

(2) Für die Zwecke des Absatzes 1 bewertet die federführende Überwachungsbehörde, ob jeder kritische IKT-Drittdienstleister über umfassende, fundierte und wirksame Vorschriften, Verfahren, Mechanismen und Vorkehrungen für das Management der IKT-Risiken verfügt, die er für Finanzunternehmen mit sich bringen kann.

Bei der in Unterabsatz 1 genannten Bewertung stehen vor allem IKT-Dienstleistungen im Mittelpunkt, die von dem kritischen IKT-Drittdienstleister bereitgestellt werden und kritische oder wichtige Funktionen von Finanzunternehmen unterstützen. Diese Bewertung wird auf IKT-Dienstleistungen, die andere als kritische oder wichtige Funktionen unterstützen, ausgeweitet, wenn dies zur Bewältigung aller relevanten Risiken erforderlich ist.

(3) Die in Absatz 2 genannte Bewertung erstreckt sich auf

a) IKT-Anforderungen, um insbesondere die Sicherheit, Verfügbarkeit, Kontinuität, Skalierbarkeit und Qualität der Dienste zu gewährleisten, die der kritische IKT-Drittdienstleister für Finanzunternehmen erbringt, sowie die Fähigkeit, jederzeit hohe Standards in Bezug auf Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit der Daten aufrechtzuerhalten;

b) die physische Sicherheit, die zur Gewährleistung der IKT-Sicherheit beiträgt, darunter auch die Sicherheit von Räumlichkeiten, Einrichtungen und Datenzentren;

c) Risikomanagementprozesse, einschließlich Strategien für IKT-Risikomanagement, IKT-Geschäftsfortführungsleitlinie und IKT-Reaktions- und Wiederherstellungsplänen;

d) Governance-Regelungen, einschließlich einer Organisationsstruktur mit klaren, transparenten und kohärenten Zuständigkeits- und Rechenschaftspflichten, die ein wirksames IKT-Risikomanagement ermöglichen;

e) die Ermittlung, Überwachung und unverzügliche Meldung wesentlicher IKT-bezogener Vorfälle an die Finanzunternehmen sowie den Umgang mit und die Lösung dieser Vorfälle, insbesondere Cyberangriffe;

f) Mechanismen für Datenübertragbarkeit, Übertragbarkeit von Anwendungen und Interoperabilität, die eine wirksame Wahrnehmung von Kündigungsrechten durch die Finanzunternehmen gewährleisten;

g) Tests von IKT-Systemen, Infrastrukturen und Kontrollen;

h) IKT-Audits;

i) die Übernahme einschlägiger nationaler und internationaler Normen, die auf die Erbringung der IKT-Dienstleistungen für Finanzunternehmen anwendbar sind.

(4) Die federführende Überwachungsbehörde nimmt auf der Grundlage der in Absatz 2 genannten Bewertung und in Abstimmung mit dem in Artikel 34 Absatz 1 genannten gemeinsamen Überwachungsnetz (Joint Oversight Network — JON) einen klaren, detaillierten und durchdachten individuellen Überwachungsplan an, in dem die für jeden kritischen IKT-Drittdienstleister vorgesehenen jährlichen Überwachungsziele und wichtigsten Überwachungsmaßnahmen beschrieben werden. Dieser Plan wird dem kritischen IKT-Drittdienstleister jedes Jahr übermittelt.

Vor der Annahme des Überwachungsplans übermittelt die federführende Überwachungsbehörde dem kritischen IKT-Drittdienstleister den Entwurf des Überwachungsplans.

Nach Eingang des Entwurfs des Überwachungsplans kann der kritische IKT-Drittdienstleister innerhalb von 15 Kalendertagen eine begründete Erklärung vorlegen, in der die erwarteten Auswirkungen auf Kunden, bei denen es sich um nicht in den Anwendungsbereich dieser Verordnung fallende Unternehmen handelt, aufgezeigt werden und gegebenenfalls Lösungen zur Risikominderung enthalten sind.

(5) Sobald die in Absatz 4 genannten jährlichen Überwachungspläne angenommen und den kritischen IKT-Drittdienstleistern übermittelt wurden, dürfen die zuständigen Behörden Maßnahmen in Bezug auf diese kritischen IKT-Drittdienstleister nur im Einvernehmen mit der federführenden Überwachungsbehörde ergreifen.

Artikel 34

Operative Zusammenarbeit zwischen den federführenden Überwachungsbehörden

(1) Um einen kohärenten Ansatz bei den Überwachungstätigkeiten sicherzustellen und um koordinierte allgemeine Überwachungsstrategien und kohärente operative Ansätze und Arbeitsmethoden sicherzustellen, richten die drei gemäß Artikel 31 Absatz 1 Buchstabe b benannten federführenden Überwachungsbehörden ein JON ein, um sich in den Vorbereitungsphasen untereinander abzustimmen und die Überwachung über die von ihnen jeweils überwachten kritischen IKT-Drittdienstleister sowie über das etwaige Vorgehen, das gemäß Artikel 42 erforderlich sein könnte, zu koordinieren.

(2) Für die Zwecke von Absatz 1 erstellen die federführenden Überwachungsbehörden ein gemeinsames Überwachungsprotokoll, in dem die genauen Verfahren für die tägliche Koordinierung und die Gewährleistung eines raschen Austauschs und rascher Reaktionen festgelegt sind. Das Protokoll wird regelmäßig überarbeitet, um den operativen Erfordernissen, insbesondere der Entwicklung praktischer Überwachungsregelungen, Rechnung zu tragen.

(3) Die federführenden Überwachungsbehörden können die EZB und die ENISA auf Ad-hoc-Basis ersuchen, fachliche Beratung zu leisten, praktische Erfahrungen auszutauschen oder an spezifischen Koordinierungssitzungen des JON teilzunehmen.

Artikel 35

Befugnisse der federführenden Überwachungsbehörde

(1) Die federführende Überwachungsbehörde hat zur Wahrnehmung der in diesem Abschnitt dargelegten Aufgaben in Bezug auf die kritischen IKT-Drittdienstleister die Befugnis,

a) alle einschlägigen Informationen und Unterlagen gemäß Artikel 37 anzufordern;

b) allgemeine Untersuchungen und Inspektionen gemäß den Artikeln 38 bzw. 39 durchzuführen;

c) nach Abschluss der Überwachungstätigkeiten Berichte anzufordern, in denen die ergriffenen Maßnahmen oder die Abhilfemaßnahmen aufgeführt sind, die von den kritischen IKT-Drittdienstleistern in Bezug auf die in Buchstabe d dieses Absatzes genannten Empfehlungen ergriffen wurden;

d) Empfehlungen zu den in Artikel 33 Absatz 3 genannten Bereichen abzugeben, insbesondere in Bezug auf Folgendes:

   i) die Anwendung spezifischer IKT-Sicherheits- und Qualitätsanforderungen oder -verfahren, insbesondere in Bezug auf die Herausgabe von Patches, Aktualisierungen, Verschlüsselung und andere Sicherheitsmaßnahmen, die die federführende Überwachungsbehörde für die Gewährleistung der IKT-Sicherheit von Diensten, die Finanzunternehmen bereitgestellt werden, für relevant hält;

   ii) die Verwendung von Bedingungen — einschließlich ihrer technischen Umsetzung — zu denen die kritischen IKT-Drittdienstleister IKT-Dienstleistungen für Finanzunternehmen bereitstellen, die die federführende Überwachungsbehörde für relevant hält, um die Entstehung punktueller Ausfälle oder deren Verstärkung zu verhindern oder um mögliche systemische Auswirkungen im Finanzsektor der Union im Falle eines IKT-Konzentrationsrisikos zu minimieren;

   iii) jede geplante Unterauftragsvergabe, in deren Fall die federführende Überwachungsbehörde aufgrund der Prüfung der gemäß den Artikeln 37 und 38 erlangten Informationen der Auffassung ist, dass eine weitere Unterauftragsvergabe, einschließlich Vereinbarungen über die Unterauftragsvergabe, die die kritischen IKT-Drittdienstleister mit anderen IKT-Drittdienstleistern oder mit IKT-Unterauftragnehmern mit Sitz in einem Drittland zu schließen beabsichtigen, Risiken für die Erbringung von Dienstleistungen durch das Finanzunternehmen oder Risiken für die Finanzstabilität mit sich bringen kann;

   iv) von der Vereinbarung über weitere Unterauftragsvergabe abzusehen, wenn die folgenden kumulativen Bedingungen erfüllt sind:

      — Bei dem ausgewählten Unterauftragnehmer handelt es sich um einen IKT-Drittdienstleister oder einen IKT-Unterauftragnehmer mit Sitz in einem Drittland;

      — die Unterauftragsvergabe betrifft eine kritische oder wichtige Funktion des Finanzunternehmens; und

— die federführende Überwachungsbehörde ist der Ansicht, dass diese Unterauftragsvergabe ein eindeutiges und ernstes Risiko für die Finanzstabilität der Union oder für Finanzunternehmen darstellt, einschließlich der Fähigkeit von Finanzunternehmen, Aufsichtsanforderungen zu erfüllen.

Für die Zwecke der Ziffer iv des vorliegenden Buchstabens übermitteln IKT-Drittdienstleister der federführenden Überwachungsbehörde unter Verwendung der in Artikel 41 Absatz 1 Buchstabe b genannten Vorlage Informationen über die Unterauftragsvergabe.

(2) Bei der Ausübung der in diesem Artikel genannten Befugnisse geht die federführende Überwachungsbehörde wie folgt vor:

a) Sie sorgt für eine regelmäßige Abstimmung innerhalb des JON und bemüht sich gegebenenfalls insbesondere um kohärente Herangehensweisen für die Überwachung kritischer IKT-Drittdienstleister;

b) sie trägt dem durch die Richtlinie (EU) 2022/2555 geschaffenen Rahmen gebührend Rechnung und konsultiert erforderlichenfalls die gemäß der genannten Richtlinie benannten oder eingerichteten zuständigen Behörden, um eine Überschneidung von technischen und organisatorischen Maßnahmen zu vermeiden, die gemäß der genannten Richtlinie auf kritische IKT-Drittdienstleister angewandt werden könnten;

c) sie ist bestrebt, das Risiko einer Störung der Dienste, die von kritischen IKT-Drittdienstleistern für Kunden bereitgestellt werden, bei denen es sich um nicht in den Anwendungsbereich dieser Verordnung fallende Unternehmen handelt, so weit wie möglich zu minimieren.

(3) Die federführende Überwachungsbehörde konsultiert das Überwachungsforum, bevor sie die in Absatz 1 genannten Befugnisse ausübt.

Bevor die federführende Überwachungsbehörde Empfehlungen gemäß Absatz 1 Buchstabe d abgibt, bietet die sie dem IKT-Drittdienstleister Gelegenheit, innerhalb von 30 Kalendertagen einschlägige Informationen bereitzustellen, mit denen die erwarteten Auswirkungen auf Kunden, bei denen es sich um nicht in den Anwendungsbereich dieser Verordnung fallende Unternehmen handelt, aufgezeigt werden und die gegebenenfalls Lösungen zur Risikominderung enthalten.

(4) Die federführende Überwachungsbehörde unterrichtet das JON über das Ergebnis der Ausübung der in Absatz 1 Buchstaben a und b genannten Befugnisse. Sie übermittelt die in Absatz 1 Buchstabe c genannten Berichte unverzüglich dem JON und den Behörden, die für diejenigen Finanzunternehmen, die die IKT-Dienstleistungen des betreffenden kritischen IKT-Drittdienstleisters in Anspruch nehmen, zuständig sind.

(5) Kritische IKT-Drittdienstleister arbeiten nach Treu und Glauben mit der federführenden Überwachungsbehörde zusammen und unterstützen sie bei der Erfüllung ihrer Aufgaben.

(6) Bei vollständiger oder teilweiser Nichteinhaltung der Maßnahmen, die infolge der Ausübung der Befugnisse gemäß Absatz 1 Buchstaben a, b oder c zu ergreifen sind, und nach Ablauf einer Frist von mindestens 30 Kalendertagen ab dem Tag, an dem der kritische IKT-Drittdienstleister eine Mitteilung über die betreffenden Maßnahmen erhalten hat, erlässt die federführende Überwachungsbehörde eine Entscheidung über die Verhängung eines Zwangsgelds, um den kritischen IKT-Drittdienstleister zur Einhaltung dieser Maßnahmen zu zwingen.

(7) Das in Absatz 6 genannte Zwangsgeld wird täglich bis zur Einhaltung der Vorschriften und für höchstens sechs Monate nach Mitteilung der Entscheidung über die Verhängung eines Zwangsgelds an den kritischen IKT-Drittdienstleister verhängt.

(8) Die Höhe des Zwangsgelds, berechnet ab dem in der Entscheidung über die Verhängung des Zwangsgelds genannten Zeitpunkt, beträgt bis zu 1 % des durchschnittlichen weltweiten Tagesumsatzes, den der kritische IKT-Drittdienstleister im vorangegangenen Geschäftsjahr erzielt hat. Bei der Festsetzung der Höhe des Zwangsgelds berücksichtigt die federführende Überwachungsbehörde in Bezug auf die Nichteinhaltung der in Absatz 6 genannten Maßnahmen folgende Kriterien:

a) Schwere und Dauer der Nichteinhaltung;

b) ob die Nichteinhaltung vorsätzlich oder fahrlässig begangen wurde;

c) das Ausmaß der Zusammenarbeit des IKT-Drittdienstleisters mit der federführenden Überwachungsbehörde.

Für die Zwecke des Unterabsatzes 1 führt die federführende Überwachungsbehörde Konsultationen im Rahmen des JON durch, um einen konsistenten Ansatz sicherzustellen.

(9) Zwangsgelder sind administrativer Art und vollstreckbar. Die Zwangsvollstreckung erfolgt nach den geltenden Vorschriften des Zivilprozessrechts des Mitgliedstaats, in dessen Hoheitsgebiet Inspektionen und Zugang erfolgen. Die Gerichte des betreffenden Mitgliedstaats sind für Beschwerden im Zusammenhang mit vorschriftswidrigem Vollzug zuständig. Die Beträge der Zwangsgelder werden dem Gesamthaushaltsplan der Europäischen Union zugewiesen.

(10) Die federführende Überwachungsbehörde veröffentlicht sämtliche verhängten Zwangsgelder, sofern dies die Stabilität der Finanzmärkte nicht ernsthaft gefährdet und den Beteiligten daraus kein unverhältnismäßiger Schaden erwächst.

(11) Die federführende Überwachungsbehörde gibt den Vertretern des dem Verfahren unterliegenden kritischen IKT-Drittdienstleisters vor Verhängung eines Zwangsgeldes nach Absatz 6 Gelegenheit, zu den Feststellungen angehört zu werden, und stützt ihre Entscheidungen ausschließlich auf Feststellungen, zu denen sich der vom Verfahren betroffene kritische IKT-Drittdienstleister äußern konnte.

Die Verteidigungsrechte der vom Verfahren betroffenen Personen werden während des Verfahrens in vollem Umfang gewahrt. Der dem Verfahren unterworfene IKT-Drittdienstleister hat, vorbehaltlich des berechtigten Interesses anderer Personen an der Wahrung ihrer Geschäftsgeheimnisse, ein Recht auf Akteneinsicht. Vom Recht auf Akteneinsicht ausgenommen sind vertrauliche Informationen sowie interne vorbereitende Unterlagen der federführenden Überwachungsbehörde.

Artikel 36

Ausübung der Befugnisse der federführenden Überwachungsbehörde außerhalb der Union

(1) Wenn sich die Überwachungsziele im Wege der Interaktion mit dem für die Zwecke des Artikels 31 Absatz 12 gegründeten Tochterunternehmen oder durch Überwachungstätigkeiten an Standorten in der Union nicht erreichen lassen, kann die federführende Überwachungsbehörde an allen Standorten in einem Drittland, die sich im Eigentum eines kritischen IKT-Drittdienstleisters befinden oder von ihm zur Erbringung von Dienstleistungen für Finanzunternehmen der Union in irgendeiner Weise im Zusammenhang mit seiner Geschäftstätigkeit, seinen Funktionen oder seinen Dienstleistungen genutzt werden, wozu alle Verwaltungs-, Geschäfts- oder Betriebsstellen, Räumlichkeiten, Grundstücke, Gebäude oder andere Immobilien gehören, die Befugnisse ausüben, die in folgenden Bestimmungen genannt werden:

a) in Artikel 35 Absatz 1 Buchstabe a und

b) in Artikel 35 Absatz 1 Buchstabe b im Einklang mit Artikel 38 Absatz 2 Buchstaben a, b und d sowie in Artikel 39 Absatz 1 und Absatz 2 Buchstabe a.

Die in Unterabsatz 1 genannten Befugnisse können unter den folgenden Bedingungen ausgeübt werden:

i) Die federführende Überwachungsbehörde erachtet die Durchführung einer Inspektion in einem Drittland als notwendig, damit sie ihre Aufgaben entsprechend dieser Verordnung vollständig und wirksam wahrnehmen kann;

ii) die Inspektion in einem Drittland steht in direktem Zusammenhang mit der Bereitstellung von IKT-Dienstleistungen für Finanzunternehmen in der Union;

iii) der betreffende kritische IKT-Drittdienstleister stimmt der Durchführung einer Inspektion in einem Drittland zu; und

iv) die einschlägige Behörde des betreffenden Drittlands wurde von der federführenden Überwachungsbehörde offiziell unterrichtet und hat keine Einwände dagegen erhoben.

(2) Unbeschadet der jeweiligen Zuständigkeiten der Organe der Union und der Mitgliedstaaten schließen die EBA, die ESMA oder die EIOPA für die Zwecke des Absatzes 1 Vereinbarungen über die Verwaltungszusammenarbeit mit der einschlägigen Behörde des Drittlands, um die reibungslose Durchführung von Inspektionen in dem betreffenden Drittland durch die federführende Überwachungsbehörde und ihr für ihren Auftrag in diesem Drittland benanntes Team zu ermöglichen. Diese Kooperationsvereinbarungen begründen keine rechtlichen Verpflichtungen gegenüber der Union und ihren Mitgliedstaaten und hindern die Mitgliedstaaten und ihre zuständigen Behörden nicht daran, bilaterale oder multilaterale Vereinbarungen mit diesen Drittländern und deren einschlägigen Behörden zu schließen.

In den Kooperationsvereinbarungen sind mindestens die folgenden Elemente festgelegt:

a) die Verfahren für die Koordinierung der im Rahmen dieser Verordnung durchgeführten Überwachungstätigkeiten und jede entsprechende Überwachung des IKT-Drittparteienrisikos im Finanzsektor durch die einschlägige Behörde des betreffenden Drittlands, einschließlich der Einzelheiten für die Übermittlung der Zustimmung dieser Behörde, damit die federführende Überwachungsbehörde und ihr benanntes Team in dessen Hoheitsgebiet allgemeine Untersuchungen und Vor-Ort-Inspektionen gemäß Absatz 1 Unterabsatz 1 durchführen können;

b) der Mechanismus für die Übermittlung aller relevanten Informationen zwischen der EBA, der ESMA oder der EIOPA und der einschlägigen Behörde des betreffenden Drittlands, insbesondere im Zusammenhang mit Informationen, die von der federführenden Überwachungsbehörde gemäß Artikel 37 angefordert werden können;

c) die Mechanismen für die unverzügliche Unterrichtung der EBA, der ESMA oder der EIOPA durch die einschlägige Behörde des betreffenden Drittlands über Fälle, in denen einem IKT-Drittdienstleister mit Sitz in einem Drittland, der gemäß Artikel 31 Absatz 1 Buchstabe a als kritisch eingestuft wurde, ein Verstoß gegen die Anforderungen zur Last gelegt wird, die er nach dem geltenden Recht des betreffenden Drittlands bei der Erbringung von Dienstleistungen für Finanzinstitute in diesem Drittland einhalten muss, sowie die angewandten Rechtsbehelfe und verhängten Sanktionen;

d) die regelmäßige Übermittlung von Neuerungen im Bereich der regulatorischen und aufsichtlichen Entwicklungen bei der Überwachung des IKT-Drittparteienrisikos für Finanzinstitute in dem betreffenden Drittland;

e) die Einzelheiten, die erforderlichenfalls die Teilnahme eines Vertreters der zuständigen Drittlandsbehörde an den Inspektionen der federführenden Überwachungsbehörde und des benannten Teams ermöglichen.

(3) Ist die federführende Überwachungsbehörde nicht in der Lage, die in den Absätzen 1 und 2 genannten Überwachungstätigkeiten außerhalb der Union durchzuführen, so

a) übt sie ihre Befugnisse nach Artikel 35 auf der Grundlage aller ihr bekannten Tatsachen und zur Verfügung stehenden Unterlagen aus;

b) dokumentiert und erläutert sie alle Folgen, die sich daraus ergeben, dass sie nicht in der Lage ist, die geplanten Überwachungstätigkeiten gemäß diesem Artikel durchzuführen.

Die in Buchstabe b genannten potenziellen Folgen werden in den Empfehlungen der federführenden Überwachungsbehörde gemäß Artikel 35 Absatz 1 Buchstabe d berücksichtigt.

Artikel 37

Auskunftsersuchen

(1) Die federführende Überwachungsbehörde kann von kritischen IKT-Drittdienstleistern durch einfaches Ersuchen oder durch Beschluss verlangen, alle Informationen zur Verfügung zu stellen, die die federführende Überwachungsbehörde benötigt, um ihre Aufgaben im Rahmen dieser Verordnung wahrzunehmen, einschließlich aller relevanten Geschäfts- oder Betriebsunterlagen, Verträge, Leit- und Richtlinien, Dokumentationen, Meldungen über IKT-Sicherheitsprüfungen, Berichte über IKT-bezogene Vorfälle sowie aller Informationen über Parteien, an die der kritische IKT-Drittdienstleister betriebliche Funktionen oder Tätigkeiten ausgelagert hat.

(2) Bei der Übermittlung eines einfachen Auskunftsersuchens nach Absatz 1 verfährt die federführende Überwachungsbehörde wie folgt:

a) Sie nimmt auf diesen Artikel als Rechtsgrundlage des Ersuchens Bezug;

b) sie gibt den Zweck des Ersuchens bekannt;

c) sie erläutert, welche Informationen gefordert werden;

d) sie legt die Frist für die Vorlage der Informationen fest;

e) sie unterrichtet den Vertreter des kritischen IKT-Drittdienstleisters, von dem die Informationen angefordert werden, darüber, dass er zu deren Übermittlung zwar nicht verpflichtet ist, die vorgelegten Informationen bei freiwilliger Beantwortung des Ersuchens jedoch nicht falsch oder irreführend sein dürfen.

(3) Fordert die federführende Überwachungsbehörde durch entsprechenden Beschluss gemäß Absatz 1 Informationen an, verfährt sie wie folgt:

a) Sie nimmt auf diesen Artikel als Rechtsgrundlage des Ersuchens Bezug;

b) sie gibt den Zweck des Ersuchens bekannt;

c) sie erläutert, welche Informationen gefordert werden;

d) sie legt die Frist für die Vorlage der Informationen fest;

e) sie nennt die Zwangsgelder, die nach Artikel 35 Absatz 6 verhängt werden, wenn die geforderten Informationen unvollständig sind oder nicht innerhalb der unter Buchstabe d genannten Frist vorgelegt werden;

f) sie weist auf das Recht nach den Artikeln 60 und 61 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 hin, vor dem Beschwerdeausschuss der ESA Beschwerde gegen den Beschluss einzulegen und den Beschluss durch den Gerichtshof der Europäischen Union (im Folgenden „Gerichtshof") überprüfen zu lassen.

(4) Die Vertreter der kritischen IKT-Drittdienstleister stellen die angeforderten Informationen zur Verfügung. Ordnungsgemäß bevollmächtigte Rechtsanwälte können die Auskünfte im Namen ihrer Mandanten erteilen. Die kritischen IKT-Drittdienstleister bleiben in vollem Umfang verantwortlich, wenn die erteilten Auskünfte unvollständig, sachlich unrichtig oder irreführend sind.

(5) Die federführende Überwachungsbehörde übermittelt den für diejenigen Finanzunternehmen, die die Dienste der betreffenden kritischen IKT-Drittdienstleister nutzen, zuständigen Behörden sowie dem JON unverzüglich eine Kopie der Entscheidung, Informationen bereitzustellen.

Artikel 38

Allgemeine Untersuchungen

(1) Die federführende Überwachungsbehörde kann zur Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung mit Unterstützung des in Artikel 40 Absatz 1 genannten gemeinsamen Untersuchungsteams erforderlichenfalls Untersuchungen von kritischen IKT-Drittdienstleistern durchführen.

(2) Die federführende Überwachungsbehörde ist befugt,

a) Aufzeichnungen, Daten, Verfahren und sonstiges für die Erfüllung ihrer Aufgaben relevantes Material unabhängig von der Speicherform zu prüfen;

b) beglaubigte Kopien oder Auszüge dieser Aufzeichnungen, Daten und dokumentierten Verfahren und von sämtlichen sonstigen Materialien anzufertigen oder zu verlangen;

c) Vertreter des kritischen IKT-Drittdienstleisters vorzuladen und zur Abgabe mündlicher oder schriftlicher Erklärungen zu Sachverhalten oder Unterlagen aufzufordern, die mit Gegenstand und Zweck der Untersuchung in Zusammenhang stehen, und die Antworten aufzuzeichnen;

d) jede andere natürliche oder juristische Person zu befragen, die dieser Befragung zum Zweck der Einholung von Informationen über den Gegenstand einer Untersuchung zustimmt;

e) Aufzeichnungen von Telefongesprächen und Datenübermittlungen anzufordern.

(3) Die Bediensteten und sonstige von der federführenden Überwachungsbehörde zu Untersuchungen gemäß Absatz 1 ermächtigte Personen üben ihre Befugnisse unter Vorlage einer schriftlichen Ermächtigung aus, in der Gegenstand und Zweck der Untersuchung angegeben werden.

In der Ermächtigung sind auch die in Artikel 35 Absatz 6 vorgesehenen Zwangsgelder für den Fall anzugeben, dass die angeforderten Aufzeichnungen, Daten, dokumentierten Verfahren oder sonstigen Materialien oder die Antworten auf Fragen, die den Vertretern des IKT-Drittdienstleisters gestellt werden, nicht geliefert werden oder unvollständig sind.

(4) Die Vertreter der kritischen IKT-Drittdienstleister sind verpflichtet, sich den Untersuchungen auf der Grundlage einer Entscheidung der federführenden Überwachungsbehörde zu unterziehen. In dem Beschluss sind Gegenstand und Zweck der Untersuchung, die nach Artikel 35 Absatz 6 vorgesehenen Zwangsgelder, die nach den Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 möglichen Rechtsbehelfe sowie das Recht, den Beschluss durch den Gerichtshof überprüfen zu lassen, anzugeben.

(5) Rechtzeitig vor Beginn der Untersuchung unterrichtet die federführende Überwachungsbehörde die für diejenigen Finanzunternehmen, die die IKT-Dienstleistungen dieses kritischen IKT-Drittdienstleisters nutzen, zuständigen Behörden über die geplante Untersuchung sowie die Identität der bevollmächtigten Personen.

Die federführende Überwachungsbehörde übermittelt dem JON alle gemäß Unterabsatz 1 mitgeteilten Informationen.

Artikel 39

Inspektionen

(1) Die federführende Überwachungsbehörde kann zur Wahrnehmung ihrer Aufgaben nach dieser Verordnung mit Unterstützung der in Artikel 40 Absatz 1 genannten gemeinsamen Untersuchungsteams sämtliche Geschäftsräume, Grundstücke oder Gebäude des IKT-Drittdienstleisters, wie Hauptverwaltungen, Betriebszentren und sekundäre Räumlichkeiten, betreten und dort alle erforderlichen Vor-Ort-Inspektionen durchführen sowie außerhalb dieser Räumlichkeiten Inspektionen durchführen.

Für die Ausübung der in Unterabsatz 1 genannten Befugnisse konsultiert die federführende Überwachungsbehörde das JON.

(2) Die Bediensteten und sonstige Personen, die von der federführenden Überwachungsbehörde zur Durchführung einer Vor-Ort-Inspektion ermächtigt wurden, sind befugt,

a) diese Geschäftsräume, Grundstücke oder Gebäude zu betreten; und

b) diese Geschäftsräume, Bücher oder Aufzeichnungen für die Dauer der Inspektion und in dem für die Inspektion erforderlichen Umfang zu versiegeln.

Die Bediensteten und sonstige von der federführenden Überwachungsbehörde ermächtigten Personen üben ihre Befugnisse unter Vorlage einer schriftlichen Ermächtigung aus, in der Gegenstand und Zweck der Inspektion sowie die in Artikel 35 Absatz 6 vorgesehenen Zwangsgelder angegeben sind, die verhängt werden, wenn sich die Vertreter der betreffenden IKT-Drittdienstleister der Inspektion nicht unterziehen.

(3) Die federführende Überwachungsbehörde unterrichtet die für diejenigen Finanzunternehmen, die diesen IKT-Drittdienstleister in Anspruch nehmen, zuständigen Behörden rechtzeitig vor der Inspektion.

(4) Die Inspektionen erstrecken sich auf das gesamte Spektrum einschlägiger IKT-Systeme, -Netzwerke, -Geräte, -Informationen und -Daten, die für die Erbringung von IKT-Dienstleistungen für Finanzunternehmen verwendet werden oder dazu beitragen.

(5) Die federführende Überwachungsbehörde unterrichtet die kritischen IKT-Drittdienstleister vor jeder geplanten Vor-Ort-Inspektion mit angemessenem Vorlauf, es sei denn, eine solche Unterrichtung ist aufgrund einer Not- oder Krisensituation nicht möglich oder würde Umstände herbeiführen, unter denen die Inspektion oder das Audit nicht mehr wirksam wären.

(6) Der kritische IKT-Drittdienstleister unterzieht sich den durch Beschluss der federführenden Überwachungsbehörde angeordneten Vor-Ort-Inspektionen. In dem Beschluss sind Gegenstand, Zweck und Datum des Beginns der Inspektion, die nach Artikel 35 Absatz 6 vorgesehenen Zwangsgelder, die nach den Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 möglichen Rechtsbehelfe sowie das Recht, den Beschluss durch den Gerichtshof überprüfen zu lassen, anzugeben.

(7) Gelangen die Bediensteten und sonstige von der federführenden Überwachungsbehörde bevollmächtigte Personen zu dem Schluss, dass ein kritischer IKT-Drittdienstleister sich einer gemäß diesem Artikel angeordneten Inspektion widersetzt, unterrichtet die federführende Überwachungsbehörde den kritischen IKT-Drittdienstleister über die Folgen einer solchen Widersetzung, einschließlich der Möglichkeit der für die betreffenden Finanzunternehmen zuständigen Behörden, Finanzunternehmen zu verpflichten, die mit diesem kritischen IKT-Drittdienstleister geschlossenen vertraglichen Vereinbarungen zu kündigen.

Artikel 40

Laufende Überwachung

(1) Bei der Durchführung von Überwachungstätigkeiten, insbesondere allgemeinen Untersuchungen oder Inspektionen, wird die federführende Überwachungsbehörde von einem gemeinsamen Untersuchungsteam unterstützt, das für jeden kritischen IKT-Drittdienstleister eingerichtet wird.

(2) Das in Absatz 1 genannte gemeinsame Untersuchungsteam setzt sich aus Mitarbeitern der folgenden Behörden zusammen:

a) der ESA;

b) der jeweils zuständigen Behörden, die die Finanzunternehmen beaufsichtigen, denen der kritische IKT-Drittdienstleister IKT-Dienstleistungen erbringt;

c) der in Artikel 32 Absatz 4 Buchstabe e genannten zuständigen nationale Behörde, auf freiwilliger Basis;

d) einer zuständigen nationalen Behörde des Mitgliedstaats, in dem der kritische IKT-Drittdienstleister seinen Sitz hat, auf freiwilliger Basis.

Die Mitglieder des gemeinsamen Untersuchungsteams müssen über Fachwissen in den Bereichen IKT und operationelle Risiken verfügen. Das gemeinsame Untersuchungsteam arbeitet unter der Koordinierung eines benannten Mitarbeiters der federführenden Überwachungsbehörde („Koordinator der federführenden Überwachungsbehörde“).

(3) Innerhalb von 3 Monaten nach Abschluss einer Untersuchung oder Inspektion nimmt die federführende Überwachungsbehörde nach Konsultation des Überwachungsforums entsprechend den in Artikel 35 genannten Befugnissen an den kritischen IKT-Drittdienstleister zu richtende Empfehlungen an.

(4) Die in Absatz 3 genannten Empfehlungen werden dem kritischen IKT-Drittdienstleister und den für diejenigen Finanzunternehmen, denen er IKT-Dienstleistungen erbringt, zuständigen Behörden unverzüglich übermittelt.

Die federführende Überwachungsbehörde kann zur Erfüllung der Überwachungstätigkeiten alle einschlägigen Zertifizierungen Dritter und interne oder externe IKT-Prüfungsberichte Dritter berücksichtigen, die von dem kritischen IKT-Drittdienstleister zur Verfügung gestellt werden.

Artikel 41

Harmonisierung der Voraussetzungen für die Durchführung der Überwachungstätigkeiten

(1) Die ESA arbeiten über den Gemeinsamen Ausschuss Entwürfe technischer Regulierungsstandards aus, um Folgendes festzulegen:

a) die Informationen, die von einem IKT-Drittdienstleister in dem Antrag bereitzustellen sind, in dem gemäß Artikel 31 Absatz 11 freiwillig um Einstufung als kritisch ersucht wird;

b) Inhalt, Struktur und Format der Informationen, die IKT-Drittdienstleister gemäß Artikel 35 Absatz 1 übermitteln, offenlegen und melden müssen, einschließlich der Vorlage für die Bereitstellung von Informationen über die Vereinbarungen über die Unterauftragsvergabe;

c) die Kriterien für die Festlegung der Zusammensetzung des gemeinsamen Untersuchungsteams, bei der eine ausgewogene Beteiligung der Mitarbeiter der ESA und der jeweils zuständigen Behörden sicherzustellen ist, sowie ihrer Benennung, Aufgaben und Arbeitsvereinbarungen;

d) die Einzelheiten der von den zuständigen Behörden vorgenommenen Bewertung der Maßnahmen, die von kritischen IKT-Drittdienstleistern auf der Grundlage der Empfehlungen der federführenden Überwachungsbehörde gemäß Artikel 42 Absatz 3 ergriffen wurden.

(2) Die ESA legen der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Juli 2024 vor.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme technischer Regulierungsstandards nach Absatz 1 entsprechend dem Verfahren nach den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

Artikel 42

Folgemaßnahmen zuständiger Behörden

(1) Kritische IKT-Drittdienstleister teilen entweder der federführenden Überwachungsbehörde innerhalb von 60 Kalendertagen nach Eingang der Empfehlungen, die von der federführenden Überwachungsbehörde gemäß Artikel 35 Absatz 1 Buchstabe d abgegeben werden, ihre Absicht mit, diesen Empfehlungen Folge zu leisten, oder legen eine begründete Erklärung für die Nichtbefolgung der Empfehlungen vor. Die federführende Überwachungsbehörde übermittelt diese Informationen unverzüglich den für das betreffende Finanzunternehmen zuständigen Behörden.

(2) Die federführende Überwachungsbehörde informiert öffentlich darüber, wenn ein kritischer IKT-Drittdienstleister es versäumt, die federführende Überwachungsbehörde gemäß Absatz 1 zu unterrichten, oder wenn die Erklärung des kritischen IKT-Drittdienstleisters als nicht ausreichend erachtet wird. Die veröffentlichten Informationen enthalten die Identität des kritischen IKT-Drittdienstleisters sowie Angaben über Art und Wesen der Nichtkonformität. Diese Informationen werden auf den zum Zweck der Gewährleistung der Sensibilisierung der Öffentlichkeit relevanten und angemessenen Umfang beschränkt, es sei denn eine solche Veröffentlichung würde den Beteiligten einen unverhältnismäßigen Schaden zufügen oder das ordnungsgemäße Funktionieren und die Integrität von Finanzmärkten oder die Stabilität des Finanzsystems der Union als Ganzes oder in Teilen gefährden.

Die federführende Überwachungsbehörde unterrichtet den IKT-Drittdienstleister über diese Veröffentlichung.

(3) Die zuständigen Behörden unterrichten die betreffenden Finanzunternehmen über die Risiken, die in den Empfehlungen an kritische IKT-Drittdienstleister gemäß Artikel 35 Absatz 1 Buchstabe d festgestellt wurden.

Beim Management des IKT-Drittparteienrisikos berücksichtigen die Finanzunternehmen die in Unterabsatz 1 genannten Risiken.

(4) Ist eine zuständige Behörde der Ansicht, dass ein Finanzunternehmen die in den Empfehlungen festgestellten spezifischen Risiken bei seinem Management der IKT-Drittparteienrisiken nicht oder nicht ausreichend berücksichtigt, teilt sie dem Finanzunternehmen mit, dass innerhalb von 60 Kalendertagen nach Eingang einer solchen Mitteilung eine Entscheidung gemäß Absatz 6 getroffen werden kann, falls keine geeigneten vertraglichen Vereinbarungen zur Beseitigung dieser Risiken bestehen.

(5) Nach Eingang der in Artikel 35 Absatz 1 Buchstabe c genannten Berichte und vor einer Entscheidung gemäß Absatz 6 können die zuständigen Behörden auf freiwilliger Basis die gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden konsultieren, die für die Beaufsichtigung eines wesentlichen oder wichtigen, von der genannten Richtlinie erfassten Unternehmens, das als kritischer IKT-Drittdienstleister eingestuft wurde, zuständig sind.

(6) Im Einklang mit Artikel 50 können zuständige Behörden als letztes Mittel nach der Mitteilung und gegebenenfalls der Abstimmung gemäß den Absätzen 4 und 5 eine Entscheidung treffen, mit der sie von Finanzunternehmen verlangen, die Nutzung oder den Einsatz einer Dienstleistung, die von einem kritischen IKT-Drittdienstleister bereitgestellt wird, vorübergehend teilweise oder vollständig auszusetzen, bis die Risiken beseitigt sind, die in den an den kritischen IKT-Drittdienstleister gerichteten Empfehlungen festgestellt wurden. Die Behörden können von Finanzunternehmen erforderlichenfalls verlangen, die einschlägigen vertraglichen Vereinbarungen, die mit kritischen IKT-Drittdienstleistern geschlossen wurden, ganz oder teilweise zu kündigen.

(7) Verweigert ein kritischer IKT-Drittdienstleister die Befolgung der Empfehlungen, indem er einen anderen als den von der federführenden Überwachungsbehörde empfohlenen Ansatz wählt, und wirkt sich ein solcher abweichender Ansatz möglicherweise auf eine große Zahl von Finanzunternehmen oder einen erheblichen Teil des Finanzsektors negativ aus und haben einzelne Warnungen der zuständigen Behörden nicht zu kohärenten Ansätzen geführt, die das potenzielle Risiko für die Finanzstabilität mindern, kann die federführende Überwachungsbehörde nach Konsultation des Überwachungsforums den zuständigen Behörden gegebenenfalls unverbindliche und nicht für die Öffentlichkeit bestimmte Stellungnahmen übermitteln, um kohärente und konvergente aufsichtliche Folgemaßnahmen zu fördern.

(8) Nach Eingang der in Artikel 35 Absatz 1 Buchstabe c genannten Berichte berücksichtigen die zuständigen Behörden bei der in Absatz 6 genannten Entscheidung die Art und das Ausmaß des Risikos, das vom kritischen IKT-Drittdienstleister nicht angegangen wird, sowie die Schwere des Verstoßes unter Berücksichtigung der folgenden Kriterien: